REMARKS

Claims 54-75 were pending prior to entering this amendment. Claims 54, 55, 62-64, and 71 have been amended. New claims 76-79 have been added. Applicant requests reconsideration and allowance of the present application.

Claim Rejections Under 35 U.S.C. § 103

Claims 62-64, 66, and 69-75 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Devine, *et al.*, (U.S. Patent 6,606,708) in view of Riggins (U.S. Patent 7,287,271), and further in view of Brown, *et al.*, (U.S. Patent 5,941,947).

No amendments have been made to claim 72. The Office Action does not provide any specific reasoning for rejecting claim 72; instead stating that claim 72 is rejected on the same basis as claim 62. However, claim 72 has a different claim scope than claim 62 and thus the reasoning for rejecting claim 62 cannot be relied on for rejecting claim 62. *See* numerous claim features of claim 72 that are absent and/or different from claim 62, e.g. "an apparatus to log onto an Operating System (OS) of the server", "[said logon] using a single Operating System (OS) level account that is established on the server", and "while remaining logged onto the server using the single OS level account, forward the filtered commands from the different users over the connection to the server", etc. Moreover, not only is specific reasoning for rejecting claim 72 omitted from the Office Action, none of the references alone, or in any combination, teach the features of claim 72.

Devine teaches a firewall 16 that restricts access to an enterprise system. *See* FIG. 1. A firewall is a network device that is "*designated as a buffer between any connected public networks and a private network...[using] lists and other methods to ensure the security of the private network.*" *See* www.cisco.com/en/US/docs/internetworking/terms_acronyms/ita.html. It is neither implied by the meaning of the term firewall, nor disclosed in any portion of Devine, that the firewall 16 logs onto the enterprise server when acting as sueh a buffer.

Even if the firewall 16 did log onto the enterprise server in some general way (which it does not for the reasons explained above), *the firewall 16 does not logon to an Operating System (OS) of the enterprise server.*

Even if Devine's firewall 16 did log onto an OS of the enterprise server in some general way (which it does not in any way log onto the enterprise server as explained above), the firewall 16 does not log onto the enterprise server as elaimed. Namely, the firewall 16 does not log onto the enterprise server using a single Operating System (OS) level account that is established on the enterprise server.

Even if Devine's firewall 16 did log onto an Operating System (OS) as claimed, Devine still does not disclose the firewall 16 remaining logged onto the enterprise server while forwarding the filtered commands from the different users over the connection to the server. Riggins does not cure these deficiencies as indicated in the Office Action.

Brown does not cure the deficiencies of Devine. Referring to F1G. 1, Brown's gateway 140 does not perform any of the claimed functionality discussed above. Accordingly, there is no gateway functionality that could have been integrated into Devine's gateway (firewall 16) to cure the deficiencies described above.

Moreover, Brown's non-gateway devices, such as access rights database 152, at least do not "log onto an Operating System (OS) of the server using a single Operating System (OS) level account that is established on the server, and while remaining logged onto the server using the single OS level account, to forward the filtered commands from the different users over thc connection to the server." Even if the aecess rights database 152 did include the claimed features (which it does not), therc is a question as to why one would have had a reason to integrate database management functions of database 152 into Devine's firewall 16.

In contrast, claim 72 includes an apparatus to log onto an Operating System (OS) of the server using a single Operating System (OS) level account that is established on the server, and while remaining logged onto the server using the single OS level account, to forward the filtered commands from the different users over the connection to the server. Thus, claim 72 should be allowed. Claims 73, being dependent, should be allowed for at least the same reason. New claims 76-79 should be allowed for at least similar reasons.

No amendments have been made to claims 74 and 75. Claim 74 includes the feature of "wherein the apparatus allows the different users to eontrol the OS independently of whether a password for logging into the OS is provided to the users." Claim 75 includes the feature of "wherein the apparatus allows the server to maintain only a single OS level account and password regardless of the number of remote users." None of the cited references disclose at least these features.

The Office Action acknowledges that Devine and Riggins eaeh fail to disclose this feature. *See* the Office Action, page 14, first paragraph.

Brown states "[t]he present invention is directed generally to the problem of flexibly and efficiently controlling the aceess rights of a large number of users to... data entities." *See* Background, first sentence (emphasis added); also *see* the Field of the Invention stating "the present invention relates to computer networks in which access rights to data entities vary..." (emphasis added). Referring to FIG. 1, the access rights database 152 manages access to content and other data entities on the host data center 104.

Brown's managing of access to content and other data objects does not appear to control OS logon, nor is this stated in the cited col. 3, lines 12-20 of Brown or anywhere else. Accordingly, the users of the computers 102 cannot control an OS installed on a host computer in the data center 104 unless the computer user 102 is provided with a password for logging into the OS. Thus, the access rights server 152 does not "allow the different users to control the OS independently of whether a password for logging into the OS is provided to the users." Similarly, the access rights server 152 does not allow the server to maintain only a single OS level account and password regardless of the number of remote users."

In contrast, claim 74 includes the feature of "wherein the apparatus allows the different users to control the OS independently of whether a password for logging into the OS is provided to the users" and claim 75 includes the feature of "wherein the apparatus allows the server to maintain only a single OS level account and password regardless of the number of remote users." Thus, claims 74 and 75 should be allowed for these reasons, in addition to the reasons stated above with respect to claim 72.

Claim 62, as amended, includes the features of the content server having established thereon an OS logon account configured to allow a first range of administrative privileges to a logged on user; one or more central servers to function as a trusted proxy for the content server by remotely administering privilege management for the content sever, , the central servers to log onto the OS using the established OS logon account that provides the first range of administrative privileges; the central servers to receive, from an endpoint for the remote user, commands for controlling the content server, to filter the received commands according to the selected level of administrative privileges such that the user can be restricted to a second range of administrative privileges, the second range being a subset of the first range of administrative privileges, and to forward the filtered commands to the content server while the central server is logged onto the content server using the OS logon account having the first range of administrative privileges. The proposed combination fails to teach at least these features for similar reasons as stated with respeet to claim 72 as well as additional reasons. Claims 62-64, 66, and 69-71, being dependent, include the same features and thus should be allowed for at least the same reasons.

Claims 54-55 and 57-59 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Devine, and further in view of Riggins.

Claim 54, as amended, includes the features of "logging the local server onto the OS, said login using a first account that gives the local server unrestricted administrative access to the OS installed on the remote server, said unrestricted login being non-corresponding with the identified privilege level" and "wherein at least one of the received commands is blocked through the filtering by the local server, the blocked command being one that is permissible with unrestricted administrative access such that said filtering and sending by the local server simulates user logon using a second different account having restricted administrative privileges to the OS installed on the remote server while the local server is actually logged onto, and accessing, the remote server using the first account having unrestricted administrative privileges." The proposed combination of Device and Riggins fails to teach at least these features for similar reasons as stated with respect to claim 72 as well as additional reasons. Claims 55 and 57-59, being dependent, include the same features and thus should be allowed for at least the same reasons.

Claim 56 is rejected under 35 U.S.C. § 103(a) as being upatentable over Devine and Riggins as applied to claims 54-55 and 57-59 above, and further in view of Booth (U.S. Patent 6,345,307).

Claim 56, being dependent, includes the same features as its base claim and thus should be allowed for at least the same reasons.

Claims 60-61 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Devine and Riggins as applied to claims 54-55 and 57-59 above, and further in view of Lomet, *et al.*, (U.S. Patent 6,182,086).

Claims 60-61, being dependent, include the same features as their base claim and thus should be allowed for at least the same reasons.

Claim 65 is rejected under 35 U.S.C. § 103(a) as being upatentable over Devine, in view of Riggins, and further in view of Brown, as dicussed in claims 62-64, 66, and 69-75 above, and further in view of Booth.

Claim 65, being dependent, includes the same features as its base claim and thus should be allowed for at least the same reasons.

Claims 67-68 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Devine in view of Riggins, and further in view of Brown as dicussed in claims 62-64, 66, and 69-75 above, and further in view of Lomet.

Claims 67-68, being dependent, include the same features as their base claim and thus should be allowed for at least the same reasons.

May 6, 2008 telephone interview

A telephone interview was eonducted on May 6, 2008 between Attorney Michael Cofield and Examiner Chau Nguyen. During the telephone interview, Attorney for Applicant asked why the Examiner believes that col. 16, lines 15-21 of Devine discloses a firewall "logging into the remote server prior to sending the messages, said login conducted using an operating system level account that is selected independently of the user". Attorney for Applicant also asked the Examiner to explain what reason someone would have had to modify Devine's firewall to include such features.

The Examiner agreed to call Michael Cofield to schedule a follow up telephone interview for further discussing these and other questions after receiving the present written response to the Office Action, in the event that any novelty or obviousness rejections remained in the application after receiving the written response.

Conclusion

For the foregoing reasons, reconsideration and allowance of the application as amended is requested. The examiner is encouraged to telephone the undersigned at (503) 224-2170 if it appears that an interview would be helpful in advancing the case.

Customer No. 73552

Respectfully submitted,

STOLOWITZ FORD COWGER LLP

Michael A. Cofield
Reg. No. 54,630

STOLOWITZ FORD COWGER LLP
621 SW Morrison Street, Suite 600
Portland, OR 97205
(503) 224-2170